Response of David A. Whiteley, Executive Vice President
North American Electric Reliability Corporation
to Additional Questions from Members of the
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

November 20, 2007

Question No. 1: What were the results of the August 2007 NERC survey sent to owners and operators regarding the status of the sector's implementation of the Aurora mitigation efforts? Please provide the Committee with a copy of the survey and a narrative of the results.

Response: Survey responses were received from 133 entities. The respondents included generating plant owners, generating plant operators, transmission owners, transmission operators, and load-serving entities. The respondents ranged from very large, multistate investor-owned utilities to small municipal utilities. Responses were received from all eight reliability regions.

The results of the survey indicate 94% of the mitigation measures recommended in the June 21 ES-ISAC advisory are completed or are in progress. This 94% consists of 60% completed and 34% in progress. The remaining 6% are not being performed for a variety of reasons (not applicable due to nature of equipment, being done by another entity, could compromise reliability rather than help reliability).

The respondents indicated they are taking a prioritized approach to the mitigation measures in applying them to their facilities. All respondents with nuclear facilities indicated they have completed the mitigation measures associated with those facilities and are working on other, smaller facilities on a prioritized basis.

A copy of the survey is enclosed.

Question No. 2: If a cyber exploit of the Aurora vulnerability is imminent, how will the Electric Sector ISAC ensure the immediate implementation of mitigation efforts?

Response: The Electricity Sector (ES) ISAC would initiate the following notification steps:

- Obtain approval from the Electricity Sector Coordinating Council to escalate the Cyber Threat Alert Level to Red.
- Post the escalated level on the ES-ISAC Web site.
- Send e-mail notifications to the electric industry through distribution lists designed for notification purposes. The NERC regional entities, the reliability coordinators, and all Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) are included on the lists. Also included on the lists are government agencies (NRC, DOE, DHS, FERC, Public Safety

Canada), other critical infrastructure sector ISACs, and industry trade associations.

- The notification would recommend that the industry promptly complete the immediate mitigation measures identified in the ES-ISAC Advisory. In the case of the June 21, 2007 ES-ISAC Advisory, those mitigation measures included:
    1. Robust cyber access mechanisms
    2. Disable remote configuration change capability
    3. Disable automatic re-close function
    4. Add time delay to close function
    5. Disable remote close function

Following notification to the industry, the ES-ISAC would follow-up to monitor progress in implementing the immediate measures. The progress would be tabulated and reported to appropriate government agencies.

Question No. 3: One of the NERC standards requires an entity to identify its "critical assets" and "critical cyber assets," with the goal of ensuring that these assets are adequately protected from any potential cyber incident. Under the NERC definition, would the assets at issue in the Aurora vulnerability be considered "critical assets"?

Response: Critical assets determined using the methodology from NERC standard CIP-002-1 would include generation assets which are subject to the Aurora vulnerability. These typically will be large generators and "blackstart" generators (*i.e.*, those generators used to restart the bulk power system following a large blackout). However, not *all* generators are essential to the reliable operation of the bulk electric system, and therefore would not be included on a list of critical assets.

Question No. 4: Are the NERC CIP standards consistent with the lessons learned document issued after the August 2003 blackout?

Response: Yes. The NERC CIP Standards are consistent with the recommendations in the August 2003 blackout report.[1] There were 13 recommendations (R32 through R44) in the "physical and cyber security" section of the recommendations list in the blackout report. Of these, all of the recommendations that could properly be addressed through Reliability Standards are addressed by requirements of the CIP standards, as shown in the table below. Recommendation 36 is not a standards issue, and recommendations 37 and 39 will require research before standards can be written to fully address the recommendation.

[1] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," U.S.-Canada Power System Outage Task Force, April 5, 2004. The recommendations regarding physical and cyber security appear at pages 163-169 of the Report, which is available at: http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf.

Recommendation	Relevant CIP Standard
32 – Implement NERC IT Standards	CIP 002-009
33 – IT Management Procedures	CIP 003, 007
34 – Corporate Level IT Governance	CIP 003
35 – Manage IT System Monitoring	CIP 005, 007, 008, 009
36 – US-Canada Risk Management Study	Government Study recommendation
37 – IT Forensics and Diagnostics	CIP 004, 009 Research recommendation
38 – Assess Risk and Vulnerability	CIP 002, 005, 007
39 – Wireless and Remote Intrusion	CIP 005, Research recommendation
40 – Control Access	CIP 006
41 – Guidance for Background Checks	CIP 004
42 – Confirm Role of NERC ES-ISAC	CIP 008
43 – Establish Clear Authority	CIP 003
44 – Prevent Information Disclosure	CIP 003

Not all the recommendations in the report address topics that are relevant to NERC standards development. Recommendation R36 deals with an intergovernmental action (initiation of a U.S.-Canada risk management study), not a performance standard requirement appropriate for incorporation into a Reliability Standard. Recommendation R41 is addressed in CIP 004, although there are significant legal and jurisdictional issues contained in its implementation that would need to be resolved outside the standards development process. The subject matter of that recommendation, moreover, is addressed by an existing NERC security guideline (scheduled for update in 2008). Recommendation R42 (confirmation of NERC ES-ISAC as the central point for sharing security information and analysis) is addressed in CIP 008. The recommendation also has been addressed outside NERC's standards process through the use of an incident reporting guideline. The guideline approach is better suited for this issue due to the frequent change in reporting procedures and protocols.

Question No. 5: Do you agree with your NERC colleague Stan Johnson, who stated that this test "is not a realistic representation of how the power system would operate"?

Response: Yes. The test completed at Idaho National Lab (INL) and depicted in the video was a 30-second edited version of over three minutes of actual test. The generator in the test was a stand-alone diesel generator rated at 3.5 MW. While it is true that generators like the one in the test are connected to the grid in North America, they are not the backbone of the system and represent a very small portion of the total generating resources available. The true backbone of the system is large generators rated at 300 to 1,100 MW. These large generating units have more sophisticated protection systems that would most likely isolate the generators from the attack long before the effects (black smoke, repetitive shaking, parts falling off) shown in the video. The test at INL was conducted with the power system in an optimal configuration for an attacker to be successful. In the real power system, the power flows in a highly complex network make

a successful attack much more difficult. The power flows on the network vary from day to day depending on what equipment is in-service or out-of-service. The direction and magnitude of the flows would have to be understood and taken advantage of by the attacker. While the test at INL helped demonstrate the feasibility of a cyber attack resulting in physical damage, a more comprehensive test would be very difficult, if not impossible to conduct.

Question No. 6: Can NERC effectively conduct oversight over electric sector owners and operators, considering that NERC operates under dues received by these same companies?

Response: Yes. NERC does not operate under a system of dues, which suggests an element of voluntariness in the payments. Rather, Section 215 of the Federal Power Act, the regulations of the Federal Energy Regulatory Commission, and NERC's bylaws and rules were specifically written to preclude undue influence by electricity sector stakeholders. Within the United States, NERC is funded through assessments to load serving entities that are approved annually by FERC. Once approved, those assessments constitute a legally binding obligation to pay that is enforceable, ultimately, through federal law. FERC also approves NERC's budget each year, which specifies how funds raised by assessment will be used for NERC's various responsibilities, including enforcement. While electric sector owners and operators, along with all other electricity sector stakeholders, have the opportunity to express their views about NERC's annual budget and assessment, electricity sector stakeholders do not have decisional authority over NERC's budget or assessments. NERC's annual budget and assessments are approved, in the first instance, by NERC's independent board of trustees, and thereafter by FERC.

Question No. 7: In his testimony, Mr. Weiss recommends that NERC incorporate the NIST Framework into its CIP standards. My understanding is that the NIST Framework is still a work in progress that is still subject to further amendment, and that it is intended to serve as model guidelines for federal government agencies, not mandatory standards applicable to the private sector with enforcement and penalty provisions. If this is true, please comment on whether the NIST Framework is actually an appropriate model for electric industry CIP standards that are required under the Federal Power Act (as amended by the Energy Policy Act of 2005) to be mandatory and enforceable? Please also comment on other reasons why the NIST Framework may not be an appropriate model for the NERC standards, including the lack of a formal stakeholder process required by Sec. 215 of the Federal Power Act, enacted by Congress in 2005 to govern the development of the NERC CIP standards.

Response: The NIST Framework[2] consists of a number of documents, including Federal Information Processing Standards (FIPS) 199 and 200 (standards) and NIST Special Publications (SP) 800-60, 800-53, 800-30, 800-18, 800-53A, and 800-37 (guidance and recommendations). As with other NIST SP800 documents, NIST SP800-

[2] See document references available from http://www.csrc.nist.gov/groups/SMA/fisma/framework.html.

53, Recommended Security Controls for Federal Information Systems, is self-described as "guidance documents and recommendations"[3] to be used in support of federal agencies' compliance activities with the mandatory Federal Information Processing Standards (FIPS) that implement the Federal Information Security Management Act (FISMA) of 2002.

The NIST guidance, as it exists in its approved format, was developed in support of FISMA for conventional IT security issues relating to conventional IT use of computers – the approved NIST guidance was not developed for industrial control systems. NIST is developing revised guidance for applicability to industrial control systems (ICS), but that has not been finalized. The revised guidance is in its 'final' public draft, with comments on the draft due on December 14, 2007. NIST plans on publishing the fully revised document within two weeks of the close of the comment period. As such, the revised ICS guidance does not yet formally exist, and therefore, could not today be included in any NERC CIP standards.

One major issue with the application of the NIST standards and guidance to the private sector deals with the assessment of impact, based on a significantly broader scope than the specific focus of the NERC Standards on the reliable operation of the bulk power system. The NIST standards and guidance process requires that *all* computer-based processes be considered, even those that have no bearing on reliable operations (and which are outside the scope of Section 215 of the FPA), including administrative functions and market functions. While these may have bearing on the business processes of the effected entities, they cannot be made mandatory under the auspices of reliability standards within the scope of Section 215.

Another issue with the application of the NIST standards and guidance is the level of technical detail included in the guidance, much of which does not directly relate to bulk power system reliability. The FIPS-199 concept of a "high water mark" for security classification requires, for example, that if any one component of a system requires a medium or high level of confidentiality, *all* components of that system must be implemented with a high confidentiality without regard to the resultant impact to operations, even if that result were detrimental to reliable operations. This will result in significantly more work required to achieve and maintain compliance with the standards, without any reliability-based benefit.

While there is a formal approval process for NIST *standards*, which require the approval of the Secretary of Commerce, there does not appear to be any formal documented process for creating, revising or approving NIST *guidance*. Further, the NIST (FIPS) standards allow the inclusion by reference of other documents (*e.g.*, SP800-53). These referenced documents do not have the same level of approval required as the formal text of the standards.

[3] NIST Special Publication 800-53 rev 1, page iv, available at http://www.csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.

In contrast, Section 215 of the FPA requires that "reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards" be provided by the Electric Reliability Organization certified by FERC (*i.e.*, NERC) in developing Reliability Standards. These requirements are incorporated in FERC's rules for certification of the ERO, and in the NERC rules of procedure as approved by FERC. The NERC process requires that "[a]ll mandatory requirements of a reliability standard shall be within an element of the standard,"[4] thereby ensuring that all mandatory and enforceable standards follow the same rigorous review and approval process approved by FERC as consistent with the statutory requirements. The NERC process allows the development of guidance, but cannot make those documents binding as mandatory and enforceable standards.

Question No. 8: Concerns have been raised regarding the potential that one or more isolated cyber failures or attacks to electric distribution system assets could directly lead to more widespread failures or electric outages in the bulk power system. Please explain if the standard radial design of electric distribution systems makes such a scenario unlikely, and if it in fact enhances the ability of electric utilities to isolate the impact of such events.

Response: The distribution system is primarily a point-to-point system, with lines emanating in a radial pattern, from the local substation to the consumer. When a distribution line is taken out of service by a falling tree in an ice storm, for example, electricity no longer flows on that spoke and the consumers' lights go out. However, the problem is limited and localized. That is the nature of the distribution system -- it is local and affects a limited area.

One or more isolated cyber attacks or failures on the distribution system will have a localized and limited effect. In addition, the isolation and protection requirements of the NERC CIP standards protect the bulk power system from intrusion reaching through the distribution system to bulk power system assets. For one or more isolated cyber failures or attacks to impact the bulk power system would require a very complex, coordinated, synchronized action. It would require a knowledgeable and determined attacker to exploit a vulnerability. While technically feasible, the likelihood is low of such a scenario successfully occurring.

Question No. 9: My understanding is that the current ISA security standards and technical reports that Mr. Weiss recommends for incorporation in the NERC CIP standards are intended to be used as guidance, not to establish expectations for auditable compliance, and there are no measures or levels of noncompliance currently associated with ISA99. Levels of noncompliance would need to be created and approved before the standards could be used as mandatory and enforceable. Do you think that such measures could be developed, if such measures are even possible, and how much time would it take to develop those measures?

[4] NERC Reliability Standards Development Procedure, Version 6.1, available at ftp://ftp.nerc.com/pub/sys/all_updl/oc/stp/RSDP_V6_1_12Mar07.pdf.

Response: Much like the status of the NIST guidance for industrial control systems, the ISA standards are still a work in progress. To date, only two "technical reports" which do not contain any requirements (*i.e.*, they are "informative" and not "normative" in nature) have been approved. Because these approved documents do not contain any "normative" requirements, quantifiable measures cannot be developed for them. The ISA standards themselves are being developed in at least four parts (or volumes), and of the four publicly documented parts, one deals with establishing terminology, concepts and models, and two deal with the establishment and operations of a security program. Only the fourth part deals with "Specific Security Requirements for Industrial Automation and Control Systems."

This fourth part has just been started, so it is impossible to determine how measures, levels of noncompliance, or violation risk factors (all of which are required elements of NERC standards, and are required for the compliance program activities) could be developed for any explicit requirements contained in that standard. It is unknown how long the process to develop those measures would require.

Question No. 10: Appendix F of the NIST 800-53 standards lists at least 25 instances where an exception to compliance for Industrial Control Systems (ICS) may be taken when "the organization determines it is not feasible or advisable (e.g., adversely impacting performance, safety, reliability)". FERC has indicated that exemptions under "technically feasible" should be as limited as possible, yet it appears that incorporation of the NIST standards would allow for a very broad exemption under technical feasibility. Can you comment on this?

Response: The NIST standards do not meet the Commission's expectations.

Question No. 11: What would be the result if the electric industry was forced to implement the NIST best practices for control systems based upon SP 800-53?

Response: Any change now in cybersecurity requirements for the bulk power system would significantly retard progress toward more robust cybersecurity protections.

A requirement to adopt NIST "best practices" now would result in a suspension of the current efforts to implement the proposed NERC cybersecurity standards pending a review of the NIST standards. The result of the review would require new implementation plans and additional time.

The loss of industry compliance momentum and the delay in implementing mandatory bulk power system cybersecurity standards would be detrimental to the reliability of the bulk power system.

Question No. 12: Are owners and operators of distribution facilities included within the NERC membership? If so, regardless of the authority extended in the Energy Policy Act, doesn't it make sense that distribution facilities be included in reliability considerations?

Response: Within the United States there are approximately 3,000 entities that own or operate distribution facilities. Approximately 375 of those entities are NERC members. NERC's authority to set and enforce reliability standards is not contingent on NERC membership, but extends to owners, operators and users of the bulk power system, whether or not they are a member of NERC. NERC can and does take account of the impact of distribution facilities on the reliability of the bulk power system. NERC can exercise jurisdiction over owners, operators, and users of the bulk power system.

Question No. 13: How does NERC ensure that its members are making efforts to mitigate the Aurora vulnerability that we know exists within control systems?

Response: The Electricity Sector Information Sharing and Analysis Center (ES-ISAC) has been operated by NERC since it was formed in 2001. The ES-ISAC was created as a result of action by the U.S. Department of Energy in response to Presidential Decision Directive 63 issued in 1998. The ES-ISAC is working with the electricity sector entities to mitigate the vulnerabilities in the system by providing information about the vulnerability, recommending mitigation measures, and following up to monitor successful completion.

The ES-ISAC has worked closely with all segments and all levels in the industry to mitigate the vulnerabilities. Meetings have been held with representatives of all the major trade associations (EEI, APPA, NRECA), the CEOs of the largest companies, the Electricity Sector Coordinating Council, numerous operating level committees, and groups of technical experts.

Because the steps needed to mitigate the Aurora vulnerability are not reflected in approved reliability standards, NERC has no authority to compel those actions. Not all subjects are the appropriate topic for standards. The standards development process is by design a public and transparent one, and matters such as the Aurora vulnerability do not lend themselves to that public process. However, NERC believes the industry is demonstrating excellent judgment and cooperation in completing the implementation of the mitigation measures.

Question No. 14: In your testimony you mention that NERC as the Electric Reliability Organization (ERO) was not given authority over facilities used for distribution of electric power. Who has authority to enforce regulations over such facilities?

Response: NERC as the electric reliability organization only has enforcement authority over the bulk power system. The definition of "bulk power system" in Section 215(a)(1) of the Federal Power Act expressly excludes facilities used for local distribution. Authority over facilities used for local distribution is generally reserved to the states, and the scope of that authority varies from state to state. State public utility commissions exercise such authority to the extent the utilities are within their jurisdiction. In a number of states, municipal utilities are not within the jurisdiction of state commissions.

Question No. 15: NERC has proposed its own set of cybersecurity standards – will these standards make a difference, i.e. will they make us safer than we are today without these standards? Will there be more to do after these standards are accepted by FERC in their current form?

Response: The answer to both these questions is "yes." These standards represent a first step in a process of continually increasing the cybersecurity of the electricity industry. While some companies already meet or exceed the requirements of these standards, the vast majority of the industry is working very hard right now to meet both the letter and intent of the standards as they are written (and expected to be approved by FERC). Essentially every company has had to do some work in order to meet either the technical requirements, or provide sufficient documentation to prove during an audit that they have met the requirements. Many companies are analyzing their systems, and implementing policy-based and technical controls to significantly increase the cyber security posture, especially at their substations and power plants.

Since these standards represent a first step, there will be additional steps. Making the modifications proposed by FERC in the pending NOPR to approve the NERC Reliability Standards will be among the additional steps to be taken in this area. As the industry gains experience and confidence in implementing cybersecurity protections, and as the vendors of control systems begin to implement increased cybersecurity protections into their systems, the cybersecurity posture of the industry will increase, and additional standards can be written to ensure that all industry participants are continuing to "raise the bar" in their cybersecurity protections. NERC's rules, and a condition of accreditation by the American National Standards Institute, require that each standard be reviewed at least every five years. NERC anticipates completing the review and upgrade of all standards over a three-year period. The cybersecurity standards are scheduled for review in 2009 to asses them based on lessons learned to that point. NERC's standards development procedure provides a systematic approach to improving to the standards and documenting the basis for those improvements, and should serve as the mechanism for achieving those improvements.

The future revisions to the NERC cyber security standards will take place after the NIST guidance on security to Industrial Control Systems has been finalized, and it is likely that some of the recommendations in that guidance will be included in revised Reliability Standards. These recommendations will be analyzed and included (or not) based on their impact on the reliable operation of the bulk power system.

Question No. 16: You mentioned in your testimony that the CIP standards were developed in a rigorous process. How does NERC plan on operating if and when it must develop security standards much quicker than the rigorous standard process allows? Are there any contingency plans in place for when immediate action is necessary?

Response: NERC operates according to its Rules of Procedure that have been approved by the Federal Energy Regulatory Commission. Section 300 of the Rules of Procedure discusses the reliability standards development processes. Rule 308 acknowledges that

the current Reliability Standards Development Procedure (Version 6.1) includes a provision for approval of urgent action standards that can be completed within 60 days and emergency actions that may be further expedited. Further, Rule 309.3, Directives to Develop Standards Under Extraordinary Circumstances, stipulates the urgent approval action procedure may be utilized if necessary to meet a timetable for action required by governmental authorities or circumstances, respecting to the extent possible the provisions in the standards development process for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing reliability standards. After making a written finding that an extraordinary and immediate threat exists to bulk power system reliability or national security, the NERC independent Board of Trustees has discretion to substantially reduce the public notice and balloting periods, thus expediting the development timeframe.

When standards are implemented using the urgent action or emergency process, one of the following three actions must occur:

- If the urgent or emergency action standard is to be made permanent without substantive changes, then the standard must proceed through the regular standards development process within one year of the urgent or emergency action approval.
- If the urgent or emergency action standard is to be substantively revised or replaced by a new standard, then a request for the new or revised standard must be initiated as soon as practical after the urgent or emergency action ballot, and the standard must proceed through the regular standards development process as soon as practical within two years of the urgent or emergency action approval.
- The urgent or emergency action standard may be withdrawn through the regular standards development process within two years.

To address immediate threats, NERC can issue an “Essential Action” alert as proposed and currently pending before FERC in Rule 808.10 of NERC’s Rules of Procedure. An “Essential Action” alert identifies specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the bulk power system to take to ensure the reliability of the bulk power system. Such alerts require NERC Board approval before issuance. These alerts are not mandatory, and NERC has no enforcement authority regarding these alerts, but NERC believes they can be a very useful tool in communicating to industry participants actions that are needed on an immediate basis to protect bulk system reliability.